International Journal of Research and Applications
Jan-Mar © 2014 Transactions; 1(1): 36-39

ISSN (online): 2349-0020
http://ijraonline.com

COMPUTER SCIENCE ORIGINAL ARTICLE

A SURVEY ON ATTACKS AND DEFENSE MECHANISMS IN PHISHING

V.Ramakanth [1] , Neela Megha Shyam Desai [2] and T.Shyam Prasad [3]
[1] Assistant Professor , [2] Head, and [3] Associate Professor
[1,2,3] Department of CSE, Krishna Murthy Institute of Technology and Engineering,
[1,2,3] Affiliated to Jawaharlal Nehru Technological University, Hyderabad-501 301
[1] rklucky53@gmail.com, [2] neelamsdesai@gmail.com , [3]shyam.tprasad@gmail.com

ABSTRACT

Phishing is defined as the act of stealing an Individual's Information for the purpose of committing financial fraud and has become a significant criminal activity on the internet [1]. The convenience of online commerce has been embraced by consumers and criminals. Phishing has a negative impact on the economy through financial losses experienced by businesses and consumers. Besides this act have the adverse effects of decreasing consumer confidence in online commerce.

Key Words - Phishing, Phish, Phreaks, Hackers, man-in-the middle attacks, Trojan horse, key-loggers.

1. INTRODUCTION

Phishing or phreaking originated from the analogy that early Internet criminals used e-mail lured to "phish" for passwords and financial data from sea of Internet users. The most likely linked to popular hacker naming conventions is "phreaks" which traces back to early hackers who were involved in the hacking of telephone systems [1]. By 1996, hacked accounts were called "phish" and by 1997 phish were actively being traded between hackers as a form of electronic currency. Very soon the definition phishing as an attack has expanded and also it included access to the personal and financial data.

2. OBJECTIVES

Originally phishing was implemented as tricking users to reply the e-mails for passwords and credit card details expanded into fake websites, installation of Trojan horse key-loggers, screen captures and man-in-the-middle attacks [2]. Further the high success rate of phishers, an extension to the classic phishing scam now includes the use of fake jobsites or job offers.

3. PRESENT TREND IN PHISHING

Phishing was identified as the use of electronic mail messages, designed to look like messages from a trusted agent, such as a bank, auction site, or online commerce site. These messages usually lure the user to take some form of action, such as validating their account information. Recently, there have been several new social engineering approaches to deceive unsuspecting users [1] [3]. These include the offer to fill out a survey for an online banking site with a monetary reward if the user includes account information, and email messages claiming to be from hotel reward clubs, asking users to verify credit card information that a customer may store on the legitimate site for reservation purposes. Included in the message is a URL for the victim to use, which then directs the user to a site to enter their personal information [2]. This site is crafted to closely mimic the look and feel of the legitimate site. The information is then collected and used by the criminals. Over time, these fake emails and web sites have evolved to become more technically deceiving to casual investigation.

Recently the definition of phishing has grown to encompass a wider variety of electronic financial crimes. In addition to the widespread use of these fake email messages and web sites to lure users into divulging their personal information, we have also observed an increase in the amount of malicious code that specifically targets user account information. Once installed on a victim's computer, these programs use a variety of techniques to spy on communications with web sites and collect account information. This method differs from the technical subterfuge generally associated with phishing scams

and can be included within the definition of spyware as well.

Phishing scams have been escalating in number and sophistication with every month that goes by. A phishing attack today now targets audience sizes that range from mass-mailings to millions of email addresses around the world, through to highly targeted groups of customers that have been enumerated through security faults in small clicks-and-mortar retail websites [5]. Using a multitude of attack vectors ranging from man-in-the-middle attacks and key loggers, through to complete recreation of a corporate website, Phishers can easily fool customers into submitting personal, financial and password data. While Spam was annoying, distracting and burdensome to all its recipients, Phishing has already shown the potential to inflict serious losses of data and direct losses due to fraudulent currency transfers.

4. PHISHING ATTACK MECHANISMS

To successfully trick the customer in doing something malicious with the server or supplied page content, there are numerous methods implemented [3]. The most commonly used methods are as explained in detail below:

- Man-in-the-middle Attacks
- Hidden Attacks

4.1 MAN -IN-THE-MIDDLE ATTACKS

In this class of attack, attackers locate themselves between the customer and the real web-based application and proxy all communications between the systems [2]. From this point of view attackers can observe and record all the transactions. This form of attack is successful for both HTTP and HTTPS communications. The customer connects to the attacker's server as if it was the real site, while the attacker's server makes a simultaneous connection to the real site.

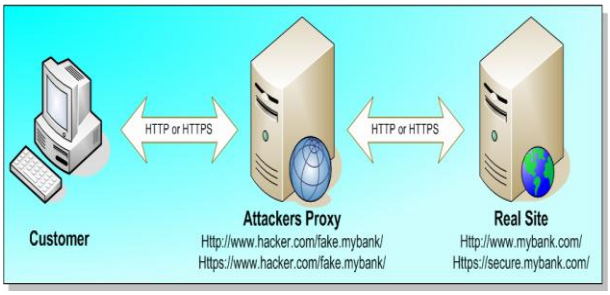

Fig 1: Man-in-the-middle attack structure

In the case of secure HTTPS communications, an SSL connection is established between the customer and the attacker's proxy while the attacker's proxy creates its own SSL connection between itself and the real server.

4.2 HIDDEN ATTACKS

An attacker may make use of HTML, DHTML and other scriptable code that can be interpreted by the customer's web browser and used to manipulate the display of the rendered information [2]. In many instances the attacker will use these techniques to disguise fake content as coming from the real site whether this is a man-in-the-middle attack or a fake copy of the site hosted on the attackers own systems.

5. MASS PHISHING ATTACKS

Mass phishing attacks have received a large amount of media attention over the last decade. An attacker sends out deceptive emails, which appear to be from a legitimate organization, to a significant number of email addresses [3]. The aim is to convince some proportion of the recipients to click on an embedded link in the message that directs them to a malicious website masquerading as a legitimate one.

More recent versions of this attack do not try to persuade the user to divulge information, but rather to persuade them to perform some action. This could be visiting a website that downloads malware through software vulnerability on the user's machine, or opening an email attachment that contains malware. If this malware were to make it onto an organization's network it could have severe consequences [4].

For instance in 2009 the Zeus Trojan was reported to have affected thousands of organizations worldwide. The approach of early mass phishing attacks was very simplistic they were produced quickly and sent to as many people as possible in the hope that a small percentage of the recipients would fall victim [5]. While crude examples of mass phishing attacks are still frequently seen, the business of phishing has been forced to evolve as increased user awareness has threatened the profits of organized criminals.

5.1 EMAIL SPOOFING

A spoofed email is one that claims to be originating from one source when it was actually sent from another. Email spoofing is a common phishing technique in which a phisher sends spoofed emails, with the sender address and other parts of the email

header altered, in order to deceive recipients. Spoofed emails usually appear to be from a website or financial institution that the recipient may have business with, so that an unsuspecting recipient would probably take actions as instructed by the email contents, such as:

- reply the email with their credit card number
- click on the link labeled as \view my statement", and enter the password when the (forged) website prompts for it
- Open an attached PDF form, and enter confidential information into the form.

5.2 WEB SPOOFING

A phisher could forge a website that looks similar to a legitimate website, so that victims may think this is the genuine website and enter their passwords and personal information, which is collected by the phisher [5]. Modern web browsers have certain built-in security indicators that can protect users from phishing scams, including domain name highlighting and https indicators. However, they are often neglected by careless users.

It is trivial to clone the look of a website by copying the front-end code; a little bit of web programming is necessary to redirect user's input into a file or database, then show a website under maintenance" notice. Users can successfully sign in and use all the services provided by the original website, while all the inputs are collected by the server, and all the pages may be modified by the server.

5.3 ATTRACTING TRAFFIC TO FORGED WEBSITE

Once a forged website is online, the phisher must make potential victims visit it. There are a few ways to do this:

- Send spoofed emails with a link to the forged website.
- Register the same domain name in a different TLD. Sometimes people will type in their country-specific TLD and expect to get a “localized" version of the website. For example, register gmail.com.cn and create a simplified-Chinese forged version of gmail.com.
- Do search engine optimization.
- Use pharming

5.4 ANTI-PHISHING

The steps you normally take to protect your computer, like using a firewall and anti-virus software, can help protect you from phishing [4]. You can review Web sites' SSL certificates and your own bank and credit card statements for an extra measure of safety.

In addition, phishers tend to leave some telltale signs in their e-mail messages and Web pages. When you read your e-mail, you should be on the lookout for:

- Threats to your account and requests for immediate action, such as "Please reply within five business days or we will cancel your account." Most companies want you as a customer and are not likely to be so quick to lose your business.
- Generic greetings, like "Dear Customer." If your bank sends you an official correspondence, it should have your full name on it. (Some phishers have moved on to spear phishing, which can include personalized information.
- Requests for personal information. Most businesses didn't ask for personal information by phone or through e-mail even before phishing became a widespread practice.
- Misspellings and poor grammar.

6. DEFENSE MECHANISMS IN PHISHING

Various techniques are developed to conduct phishing attacks and make them less suspicious. Email spoofing is used to make fraudulent emails appear to be from legitimate senders, so that recipients are more likely to believe in the message and take actions according to its instructions [4][6][7]. Web spoofing makes forged websites look similar to legitimate ones, so that users would enter confidential information into it. Pharming attracts traffic to those forged websites. Malware are installed into victims' computers to collect information directly or aid other techniques. PDF documents, which support scripting and fillable forms, are also used for phishing.

7. AWARENESS OF PHISHING

Originally the primary advantage for criminals conducting phishing-related fraud was the lack of education and awareness of the existence of financial crimes targeting internet users and the policies and procedures of online sites for contacting their customers regarding account information and maintenance issues.

Both of these issues are being addressed by the online commerce sites and the information security community though various awareness mechanisms:

- General information on phishing distributed in company email or on a company's web site
- Alerts sent to customers about phishing scams directly targeting a specific company
- Reminders to customers of corporate policies on contacting customers regarding their account
- Papers and talks from the security community targeted to users and businesses

When companies choose to implement a customer phishing awareness program, it is important that they educate employees as well [8]. In particular, the employees who interact with customers should be knowledgeable about phishing so they can answer customers' questions.

Note that we have observed the criminals attempting to take advantage of increasing awareness by phrasing their phishing emails accordingly; for example, a phishing email might state that the customer's account information may have been compromised due to a phishing scam.

Finally, a significant portion of phishing awareness efforts have focused on the threats posed by phishing emails and web sites [4]. However, there is a significant threat from malware that people need to be made aware of as well. When a phishing email or web site is properly identified by a consumer, he or she can easily correlate it with the action of trying to steal account information [6]. However, if malware is detected on a user's computer, the common response is to follow instructions on isolating and removing the threat. The user may not be aware of the functionality of the malware and thus the correlation to the action of trying to steal account information may not be clear.

8. CONCLUSIONS

Phishing started off being part of popular hacking culture. Now, as more organizations provide greater online access for their customers, professional criminals are successfully using phishing techniques to steal personal finances and conduct identity theft at a global level.

By understanding the tools and technologies Phishers have in their arsenal, businesses and their customers can take a proactive stance in defending against future attacks [5][6][7]. Organizations have within their grasp numerous techniques and processes that may be used to protect the trust and integrity of their customers personal data. The points mentioned within this paper and the solutions proposed, represent key steps in securing online services from fraudulent phishing attacks and also go a long way in protecting against many other popular hacking or criminal attack vectors. By applying a multi-tiered approach to their security model i.e. client-side, server-side and enterprise organizations can easily manage their protection technologies against today's and tomorrow's threats without relying upon proposed improvements in communication security that are unlikely to be adopted globally for many years to come.

REFERENCES

1. The Phishing Guide Understanding & Preventing Phishing Attacks by Gunter Ollmann, Director of Security Strategy.
2. IBM Internet Security Systems.
3. How Phishing Works by Tracy V. Wilson, http://computer.howstuffworks.com/phishing.htm/printable
4. The Phishing Guide Understanding & Preventing Phishing Attacks Next Generation Security Software Ltd.
5. Phishing Websites Detection based on Phishing Characteristics in the Webpage Source Code Mona Ghotaish Alkhozae, Omar Abdullah Batarfi Department of Computer Sciences, FCIT King Abdulaziz University, Jeddah, KSA
6. Implementing a Web Browser with Phishing Detection Techniques World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 7, 289-291, 2011
7. Preventing Phishing Attacks Using Trusted Computing Technology Adil Alsaid and Chris J. Mitchell.
8. Wu, M., R. Miller, & S. Garfinkel. Do Security Toolbars Actually Prevent Phishing Attacks? Posters SOUPS (2005).